Attorney Docket No. B-4271 618992-5

PATENT

AF/ITW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant: Andrew Charles David Hay	)	On Appeal to the Board of Appeals
Patent Application No.: 09/931,657	)	
Filed: 08/16/2001	)	Group Art Unit: 2173
For: "Security Apparatus"	)	Examiner: Nguyen, Cao H
	)	Date: August 14, 2006

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the Final rejection, dated February 24, 2006, for the above identified patent application. Appellants submit that this Appeal Brief is being timely filed, since the Notice of Appeal was filed on June 16, 2006. Please charge the Appeal Brief fee of $500.00 to deposit account no. 08-2025.

REAL PARTY IN INTEREST

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC

RELATED APPEALS AND INTERFERENCES

Appellants submit that there are no other prior and pending appeals, interferences or judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1-17 are currently pending. Claims 1-17 are the subject of this Appeal and are reproduced in the accompanying Claims appendix.

STATUS OF AMENDMENTS

No Amendment After Final Rejection has been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

The invention described and claimed in the present application relates to security apparatus. The embodiments of security apparatus, computer system and a methods for modifying the security status of a computer apparatus are exemplified in independent Claims 1, 6 10 and 14.

Claim 1 of the present disclosure is directed to a security apparatus comprising: means for representing to a user a plurality of components of a computer platform (501; Fig. 6; Paragraph [0061] of the present application as published); means for representing to the user interactions among the plurality of components (510; Figs. 7a-14; Paragraphs [0062]-[0093]); and means for allowing the user to modify a security setting associated with at least one of the plurality of components (Paragraphs [0095]-[0102]).

Claim 6 of the present disclosure is directed to a method for modifying the security status of a computer apparatus, the method comprising: representing to a user a plurality of components of a computer platform (501; Fig. 6; Paragraph [0061]); representing to the user interactions among the plurality of components (510; Figs. 7a-14; Paragraphs [0062]-[0093]); and allowing the user to modify a security setting associated with at least one of the plurality of components (Paragraphs [0095]-[0102]).

Claim 10 of the present disclosure is directed to a computer system, comprising: a memory (22) to store computer-readable code; and a processor (21) operatively coupled to said memory and configured to implement said computer-readable code, said computer-readable code being configured to: represent to a user a plurality of computer components (501; Fig. 6; Paragraph [0061]); represent to the user interactions among the plurality of computer components (510; Figs. 7a-14; Paragraphs [0062]-[0093]); and

allow the user to modify a security setting associated with at least one of the computer components (Paragraphs [0095]-[0102]).

Claim 14 of the present disclosure is directed to a method for modifying the security status of a computer component, the method comprising: depicting a plurality of computer components (501; Fig. 6; Paragraph [0061]); depicting interactions among the plurality of computer components (510; Figs. 7a-14; Paragraphs [0062]-[0093]); and allowing modification of a security setting associated with at least one of the computer components (Paragraphs [0095]-[0102]).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1: Whether Claims 1-17 are patentable under 35 U.S.C. 102(b) in view of Novoa, U.S. Patent No. 6,223,284, (hereinafter "Novoa")?

ARGUMENT

Issue 1: Whether Claims 1-17 are patentable under 35 U.S.C. 102(b) in view of Novoa, U.S. Patent No. 6,223,284, (hereinafter "Novoa")?

In the final Office Action of February 24, 2006, the Examiner rejects Claims 1-17 under 35 U.S.C. 102(b) as being anticipated by Novoa. Appellants respectfully disagree.

Claim 1

To start, Appellant would like to respectfully point out that the Examiner's comments on pages 2-3, rejecting Claims 1-6, pertain to claim features that have been deleted in Appellant's response dated October 4, 2004 and fail to address the claim features added with the same response. For example, the Examiner asserts that "a receiver for receiving a security metric associated with a computer entity" is disclosed by Novoa's abstract and col. 11, lines 3-22. See page 2, section 2 of the final Office Action dated February 24, 2006. As shown in the enclosed Claims Appendix, Claim 1 does not recite "a receiver for receiving a security metric associated with a computer entity." Appellant respectfully requests that the Examiner's comment on pages 2-3, pertaining to Claims 1-6, be ignored in view of the claim amendments dated October 4, 2004.

Furthermore, Appellant submits that the Examiner has not shown that Novoa discloses, suggests or teaches, *inter alia*, the following features recited by Claim 1 of the present application:

> "means for representing to a user a plurality of components of a computer platform; means for representing to the user interactions among the plurality of components; and means for allowing the user to modify a security setting associated with at least one of the plurality of components" (emphasis added)

According to Novoa, an administrator is presented with different dialog boxes as shown in Novoa's Figures 6A-6E reproduced below. Novoa teaches that the dialog box "300" of Figure 6A displays a Quick-Lock mode option for disabling a keyboard and mouse interface from within an application, a Quick-Blank mode option for blanking a video display 82 from within an application, a removable media bootability option for preventing a user from booting the computer S from the removable media drives, an option to change the administrator password, an option to change the asset tag which is a unique number or text string such as an owner's property identification number used to help track the specific computer system S, etc. See column 7, line 55 to column 8, line 10 of Novoa. After viewing the dialog box "300," the administrator is presented with further dialog boxes of Figures 6B-6D when the administrator double-clicks on any of the options in the dialog box "300." See column 8, line 33 to column 9, line 16 of Novoa. For example, Novoa displays dialog box "334," reproduced below, when the administrator double-clicks on the change the administrator password option; Novoa displays dialog box "336," reproduced below, when the administrator double-clicks on the Quick-Blank mode option; and Novoa displays dialog box "338," reproduced below, when the administrator double-clicks on the asset tag option. The administrator is further presented with a dialog box "320," reproduced below, that provides a summary of the security options for a security options template file. See column 9, lines 28-31 of Novoa.

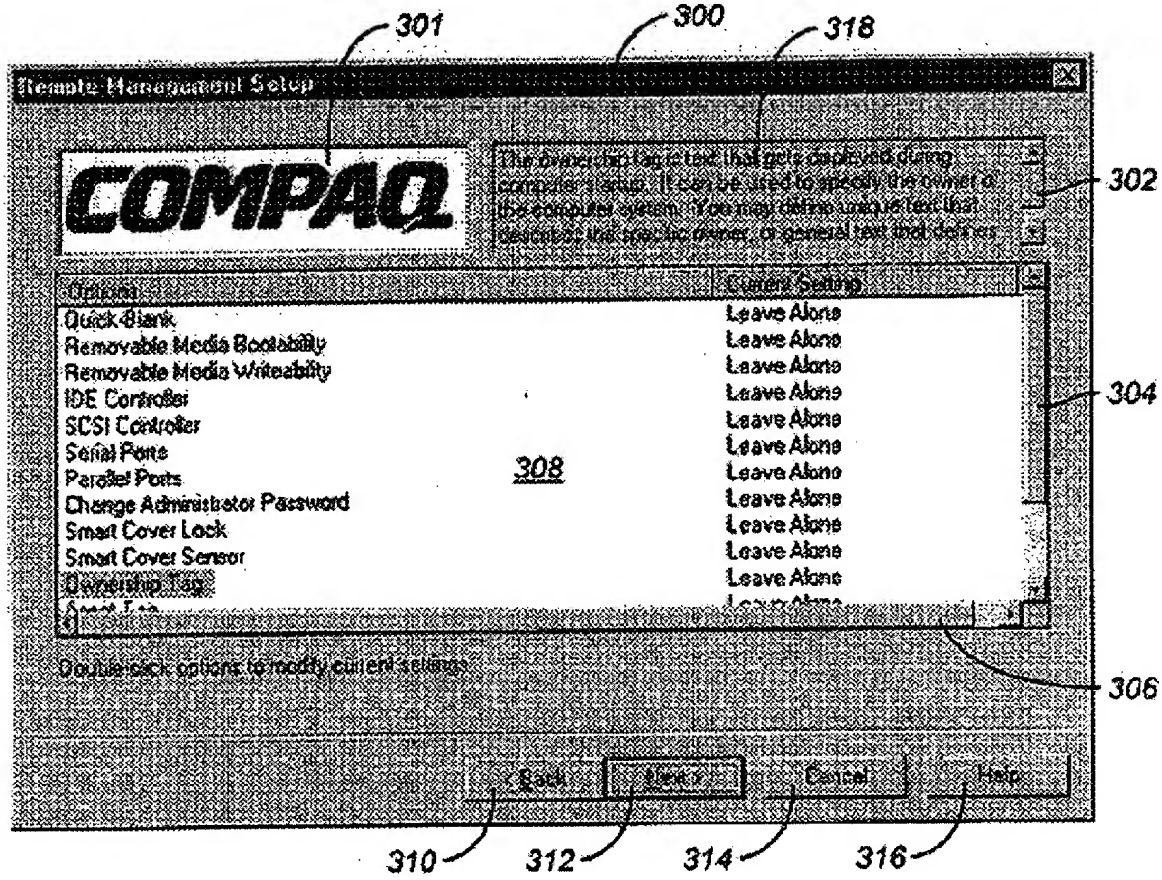

301
300
318
Remote Management Setup
COMPAQ
302
Current Setting
Quick Blank
Removable Media Bootability
Removable Media Writeability
IDE Controller
SCSI Controller
Serial Ports
Parallel Ports
Change Administrator Password
Smart Cover Lock
Smart Cover Sensor
Ownership Tag
Leave Alone
304
308
306
Double-click options to modify current settings
Back
Next >
Cancel
Help
310
312
314
316

FIG. 6A

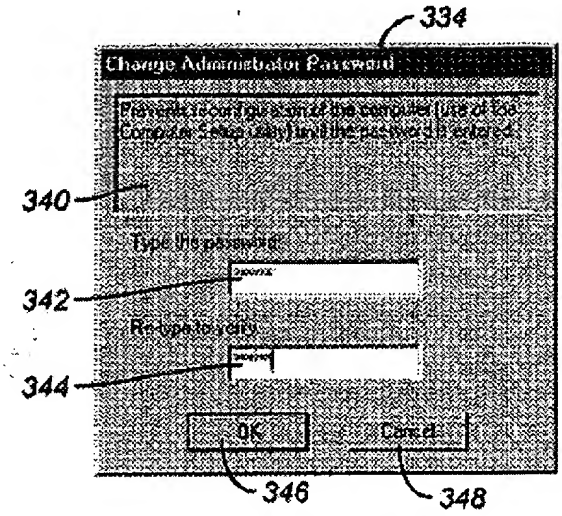


FIG. 6B

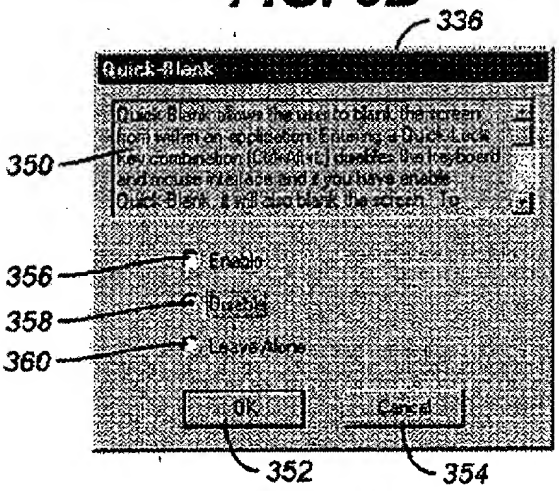


FIG. 6C

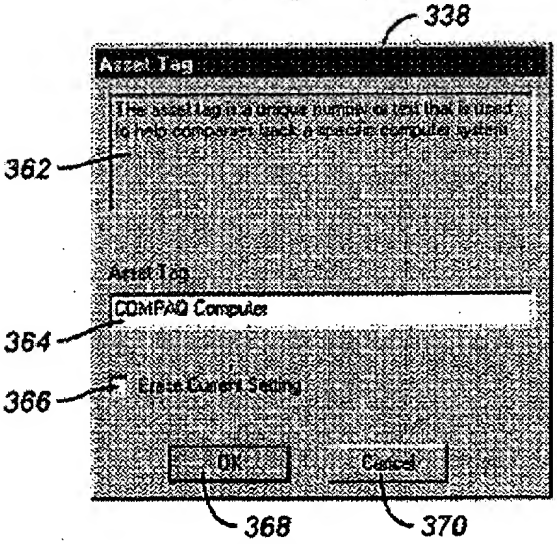


FIG. 6D

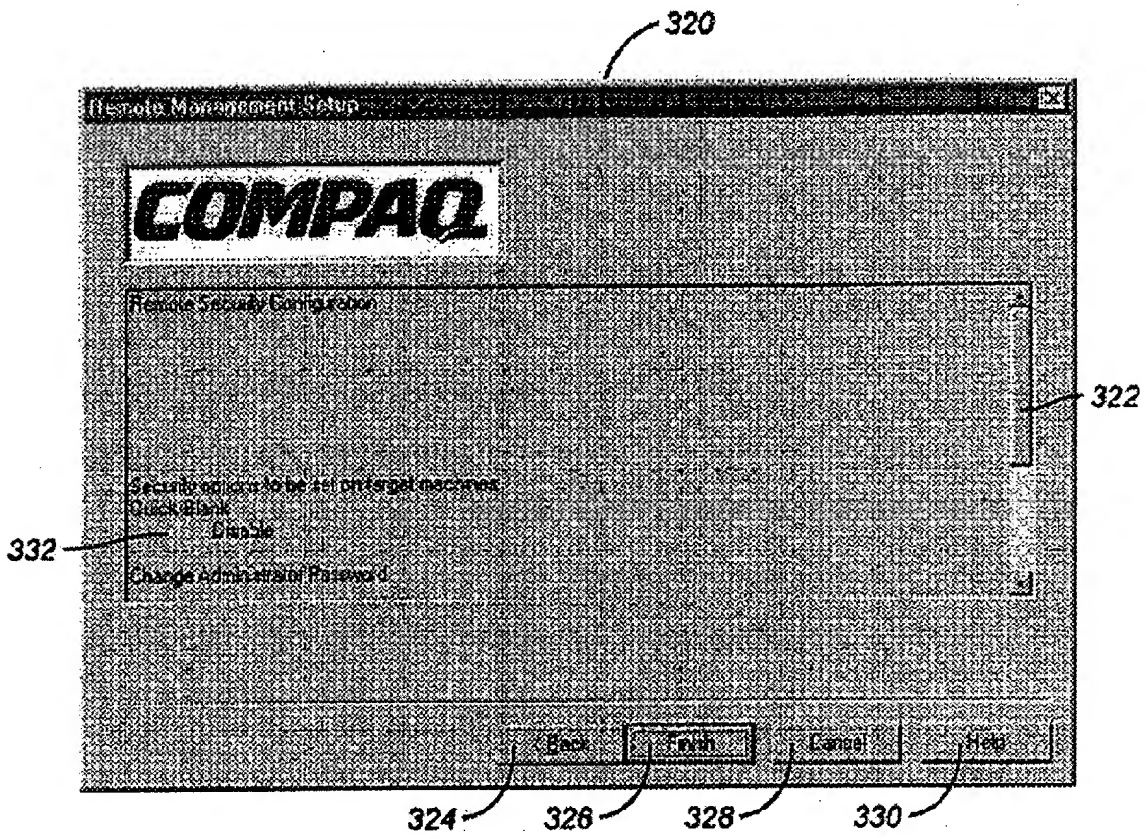


FIG. 6E

As can be seen in Novoa's Figures 6A-E reproduced above, the dialog boxes "300," "334," "336," "338," and "320" appear to be passive because they require administrator's input to change the settings in the dialog boxes and they do not show interactions among different components disclosed by Novoa.

Appellant submits that Novoa does not teach, disclose or suggest "means for representing to the user interactions among the plurality of components" (emphasis added) as recited in Claim 1, because Novoa's dialog boxes "300," "334," "336," "338," and "320" presented to the administrator allow the administrator to change the settings but do not represent to the administrator interactions among different components. Hence, Claim 1 is patentable over Novoa and the rejection should be revered on appeal.

Claims 2-5

Claims 2-5, at least based on their dependency on Claim 1, are also patentable over Novoa and the rejection should be revered on appeal.

Claim 6

Appellant submits that, at least for the reasons stated above for Claim 1, Novoa does not teach, disclose or suggest "representing to the user interactions among the plurality of components" as recited in Claim 6. Hence, Claim 6 is patentable over Novoa and the rejection should be revered on appeal.

Claim 10

Appellant submits that, at least for the reasons stated above for Claim 1, Novoa does not teach, disclose or suggest "represent to the user interactions among the plurality of computer components" as recited in Claim 10. Hence, Claim 10 is patentable over Novoa and the rejection should be revered on appeal.

Claims 11-13

Claims 11-13, at least based on their dependency on Claim 10, are also patentable over Novoa and the rejection should be revered on appeal.

Claim 14

Appellant submits that, at least for the reasons stated above for Claim 1, Novoa does not teach, disclose or suggest "depicting interactions among the plurality of computer components" as recited in Claim 10. Hence, Claim 14 is patentable over Novoa and the rejection should be revered on appeal.

Claims 15-17

Claims 15-17, at least based on their dependency on Claim 14, are also patentable over Novoa and the rejection should be revered on appeal.

* * *

Conclusion

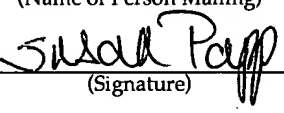
For the extensive reasons advanced above, Appellant respectfully contends that each claim is patentable. Therefore, reversal of all rejections and objections is courteously solicited.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this Appeal Brief is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this correspondence is being deposited with the United States Post Office with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22323-1450 on

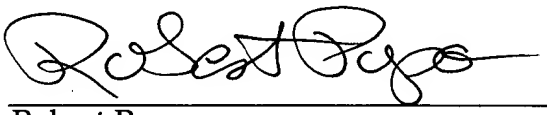
August 14, 2006
(Date of Mailing)

Susan Papp
(Name of Person Mailing)


(Signature)

August 14, 2006
(Date)

Respectfully submitted,



Robert Popa
Attorney for Appellants
Reg. No. 43,010
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300

Encl.: postcard

1. Security apparatus comprising:

means for representing to a user a plurality of components of a computer platform;

means for representing to the user interactions among the plurality of components; and

means for allowing the user to modify a security setting associated with at least one of the plurality of components.

2. Security apparatus according to claim 1, wherein the means for representing the plurality of components comprise: means for representing software and/or hardware functionality of the computer platform.

3. Security apparatus according to claim 1, further comprising input means for allowing the user to interact with the modifying means to modify the security setting.

4. Security apparatus according to claim 1, further comprising means for providing possible modifications to the security setting.

5. Security apparatus according to claim 1, wherein a level of complexity of representing to the user the plurality of components is selectable by the user.

6. Method for modifying the security status of a computer apparatus, the method comprising:

representing to a user a plurality of components of a computer platform;

representing to the user interactions among the plurality of components; and

allowing the user to modify a security setting associated with at least one of the plurality of components.

7. The method according to claim 6, wherein representing the plurality of components comprises:

representing software and/or hardware functionality of the computer platform.

8. The method according to claim 6, further comprising:

presenting to the user possible modifications to the security setting.

9. The method according to claim 6, further comprising:

allowing the user to select a level of complexity of representing to the user the plurality of components.

10. A computer system, comprising:

a memory to store computer-readable code; and

a processor operatively coupled to said memory and configured to implement said computer-readable code, said computer-readable code being configured to:

represent to a user a plurality of computer components;

represent to the user interactions among the plurality of computer components; and

allow the user to modify a security setting associated with at least one of the computer components.

11. The computer system according to claim 10, wherein representing the plurality of computer components comprises:

representing software and/or hardware functionality of a computer.

12. The computer system according to claim 10, wherein the computer-readable code is further configured to:

present the user possible modifications to the security setting.

13. The computer system according to claim 10, wherein the computer-readable code is further configured to:

allow the user to select a level of complexity of representing to the user the plurality of computer components.

14. Method for modifying the security status of a computer component, the method comprising:

depicting a plurality of computer components;

depicting interactions among the plurality of computer components; and

allowing modification of a security setting associated with at least one of the computer components.

15. The method according to claim 14, wherein depicting the plurality of computer components comprises:

depicting software and/or hardware functionality of a computer.

16. The method according to claim 14, further comprising:

presenting possible modifications to the security setting associated with one or more of the computer components.

17. The method according to claim 14, further comprising:

allowing selection of a level of complexity for displaying the plurality of computer components.

No evidence is being submitted

No copies of decisions rendered in related proceedings are being submitted.